

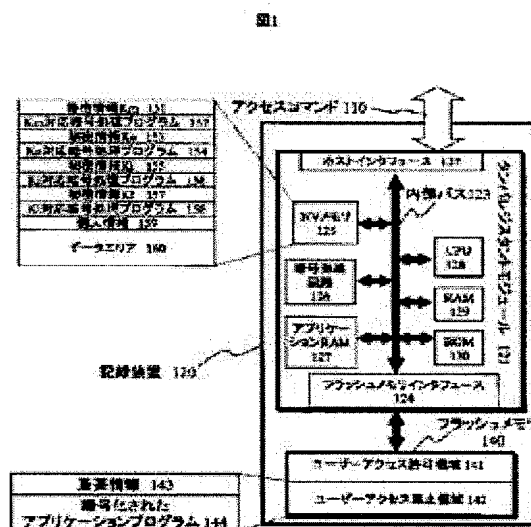
(11)Publication number : 2002-229861
(43)Date of publication of application : 16.08.2002

(21)Application number : 2001-030384
(22)Date of filing : 07.02.2001

(71)Applicant : HITACHI LTD
(72)Inventor : IGUCHI SHINYA
TSUNEHIRO TAKASHI
TSUNODA MOTOYASU
ISHIHARA HARUJI
MIZUSHIMA EIGA
TOTSUKA TAKASHI

(57)Abstract:

SOLUTION: A tamper resistant module 121 and a flash memory 140 are mounted on the recording device 120. A CPU 128 in the tamper resistant module 121 judges the secrecy of data sent by an access command 110. A small amount of data having high secrecy is recorded in an NV memory 125, a large amount of data having high secrecy is ciphered and recorded in the flash memory 130, and data having low secrecy is directly recorded in the flash memory 140.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-229861

(P2002-229861A)

(43) 公開日 平成14年8月16日 (2002.8.16)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
			3 2 0 B 5 B 0 2 5
3/06	3 0 4	3/06	3 0 4 H 5 B 0 3 5
3/08		3/08	C 5 B 0 6 5
1/00		9/06	6 6 0 D 5 B 0 7 6
審査請求 未請求 請求項の数 7 O L (全 20 頁) 最終頁に続く			

(21) 出願番号 特願2001-30384(P2001-30384)

(22) 出願日 平成13年2月7日 (2001.2.7)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 井口 慎也

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 常広 隆司

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

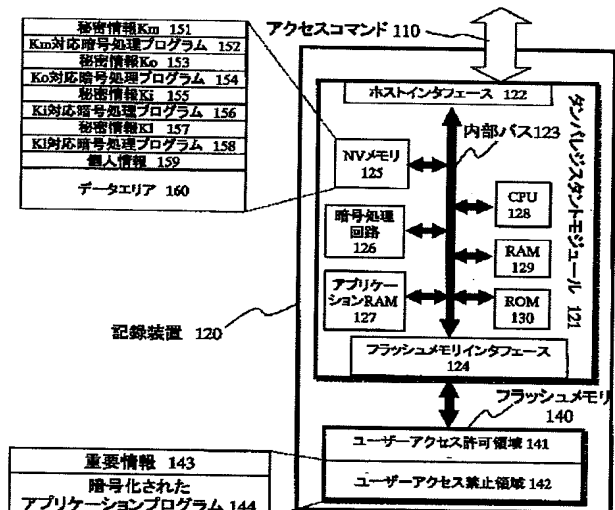
最終頁に続く

(54) 【発明の名称】 著作権保護機能つき記録装置

(57) 【要約】

【課題】本発明は、半導体メモリを用いた記録装置に、特性の違う二種類の半導体不揮発性メモリを搭載し、それらに書きこむデータを記録装置で選別することで、秘匿性の高いデータを多量に記録することが可能な、記録装置を安価に実現する。

【解決手段】記録装置120にタンパレジスタントモジュール121とフラッシュメモリ140を搭載し、アクセスコマンド110によって送信されてきたデータの秘匿性をタンパレジスタントモジュール121内のCPU128が判断し、秘匿性の高い小容量のデータをNVメモリ125へ、秘匿性の高い大容量のデータは暗号化してフラッシュメモリ140へ、そして秘匿性の低いデータをそのままフラッシュメモリ140へ記録する手段を有する記録装置。



【特許請求の範囲】

【請求項1】内部不揮発性メモリを有するメモリコントローラ及び外部不揮発性メモリとを具備し、前記メモリコントローラは、外部装置と接続されるホストインターフェイス、上記外部不揮発性メモリと接続されるメモリインターフェイス、前記ホストインターフェイスとメモリインターフェイスと接続された内部バス、前記内部バスに接続されたCPU、内部不揮発性メモリ及びアプリケーション格納用メモリとを有し、前記内部不揮発性メモリは、ユーザー個人情報であるKi、ユーザー端末装置情報であるKo、暗号化処理プログラムを外部不揮発性メモリからメモリコントローラのアプリケーション格納用メモリに復号化して格納するための情報であるKm及びアプリケーションダウンロード時の情報であるKLのいずれかの秘密情報と、前記秘密情報に対応する暗号化処理プログラムとを格納することが可能であり、前記外部不揮発性メモリは、ユーザーアクセス許可領域とユーザーアクセス禁止領域とを有し、コンテンツデータを前記ユーザーアクセス許可領域に格納し、前記メモリコントローラが使用するファームウェアを前記ユーザーアクセス禁止領域に格納することが可能であることを特徴とするパッケージされた記録装置。

【請求項2】暗号化されたアプリケーションプログラムを前記ユーザーアクセス禁止領域に格納することが可能であることを特徴とする請求項1記載のパッケージされた記録装置。

【請求項3】コマンドもしくは書込データの属性を前記メモリコントローラの前記CPUが解析して、格納先を前記外部不揮発性メモリ又は前記内部不揮発性メモリとに振り分ける機能を有することを特徴とする請求項1又は2記載のパッケージされた記録装置。

【請求項4】前記内部不揮発性メモリが容量不足か否かを前記CPUが判定して、Ki、Ko、Km及びKLのいずれかに対応する前記暗号化処理プログラムのデータもしくはそれを暗号化したデータを外部不揮発性メモリに格納することが可能であることを特徴とする請求項3記載のパッケージされた記録装置。

【請求項5】前記外部不揮発性メモリは、多値のフラッシュメモリを使用して構成されていることを特徴とする請求項1、2、3又は4記載のパッケージされた記録装置。

【請求項6】請求項1記載のパッケージされた記憶装置を実装したユーザー端末装置とサービスプロバイダが有するサーバとのデータ転送方法であって、前記ユーザー端末装置のIDであるKoを前記記録装置から前記ユーザー端末装置に送信し、前記Koを前記ユーザー端末装置から前記サービスプロバイダのサーバへ両者が保有している共通の鍵で暗号化し

て送信し、

前記サービスプロバイダのサーバで前記Koを共通の鍵で復号化して取り出して前記Koを共有し、

前記Koを利用して前記ユーザー端末装置と前記サービスプロバイダのサーバ間でデータを暗号化して送受信することで、前記ユーザー端末装置と前記サービスプロバイダのサーバ間で、第三者がデータを取り出すことができない安全な外部送信経路を確立し、

さらに、前記記録装置でKiを前記サービスプロバイダのサーバが既知の鍵で暗号化して前記ユーザー端末装置に送信し、

前記ユーザー端末装置から前記外部送信経路を通して暗号化された前記Kiを前記サービスプロバイダのサーバに送信し、

前記サービスプロバイダのサーバで復号化して前記Kiを共有し、

前記Kiを暗号化の鍵生成情報として利用することで、前記記録装置と前記サービスプロバイダのサーバとの間で安全な通信経路を確立し、

前記安全な通信経路で、前記サービスプロバイダのサーバから前記記録装置へデータを転送することを特徴とする方法。

【請求項7】請求項1、2、3、4又は請求項5に記載の記録装置を搭載可能で、前記記録装置と秘密情報Kiを共有することで暗号化された通信を行い、前記記録装置からデータを読み出し復号化して再生する機能を有するデコード回路を有するユーザー端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記憶装置及び記憶装置に接続される情報機器に関し、特に、情報機器と記録装置とのデータ転送の制御方式に関する。

【0002】

【従来の技術】近年、インターネット等のネットワーク社会の発達によって、ネットワークに流通する音楽や画像といったコンテンツの著作権を保護するための技術の重要性が高まっている。著作権保護の技術として、暗号化・復号化に使用する秘密鍵を格納する秘密鍵記憶回路と、データを保存するデータ記憶回路を搭載し、書き込み制御回路を用いて秘密鍵記憶回路に秘密鍵を書き込む機能と、相手機器を認証する機能を有するメモリICカードが提案されている。この技術は、例えば、特開2000-163547号公報に開示されている。

【0003】

【発明が解決しようとする課題】従来技術では、メモリICカード等のパッケージされた記憶装置上の記録媒体にすべてのデータが記録される。メモリICカード等のパッケージされた記憶装置は、コンテンツの盗難等を防止するため、カード外部から内部のデータを解析することが困難な構造(タンパレジスタントモジュール)を有する。

一般的に、タンパレジスタントモジュールを有するメモリICカード等のパッケージされた記憶装置は高価で、かつメモリの記憶容量が小さい。したがって、メモリICカード等のパッケージされた記憶装置に、秘匿性の高いデータを多量に格納することは非常に困難であった。

【0004】また、従来技術では、メモリICカード等のパッケージされた記憶装置では、秘匿性の高いデータと低いデータが記録装置で判断することなしに、上位装置からの転送指示に応じてそのままタンパレジスタントモジュールへ格納されていた。このため、秘匿しなくても良いデータまでタンパレジスタントモジュール内にすべて格納されることとなり、タンパレジスタントモジュール内の記憶領域を有効に活用できなかった。

【0005】また、従来技術では、データ保存用の記憶領域としてEEPROM等の不揮発性メモリ（以下NVメモリ）が使用される。しかし、従来技術で使用されるNVメモリは書き換え可能な回数が少なく、多くのコンテンツを何度も入れ替えることが困難であった。

【0006】さらに、従来技術では、上述したように、メモリICカード等のパッケージされた記憶装置の記憶容量が小容量なので、メモリICカード上でアプリケーションを実行する場合でも、プログラムの使用する記憶容量が小さいアプリケーションしか実行することが出来なかった。

【0007】本発明の目的は、秘匿性の高いデータを安価にかつ多量に何度も保存できるパッケージされた記憶装置を提供することである。

【0008】本発明の他の目的は、タンパレジスタントモジュール内の記録領域を有効利用することができる記憶装置を提供することにある。

【0009】さらに、本発明の他の目的は、様々なアプリケーションが記録され、しかも規模の大きなアプリケーションが実行できるパッケージされた記憶装置を提供することにある。

【0010】

【課題を解決するための手段】上記目的を達成するために、CPU、RAM、ROM、不揮発性メモリ及び暗号処理回路から構成されたタンパレジスタントモジュールと大容量なフラッシュメモリを用いて、タンパレジスタントモジュール内に記録装置固有の秘密鍵等を記録しておき、タンパレジスタントモジュール内の不揮発性メモリへ記録出来ない情報は、秘密鍵で暗号化したのちフラッシュメモリへ書き込む手段を備えた記録装置を構成する。

【0011】上記他の目的を達成するために、タンパレジスタントモジュール内のCPUが外部から送信されてきた情報の秘匿性を判断し、重要な情報はタンパレジスタントモジュール内部の不揮発性メモリへ記録し、通常の情報はフラッシュメモリへ記録するようにデータを振り分ける機能を搭載した記録装置を構成する。

【0012】さらに、上記他の目的を達成するために、タンパレジスタントモジュール内でアプリケーションを実行するRAMを搭載し、アプリケーションをタンパレジスタントモジュール内の秘密鍵で暗号化し外部のフラッシュメモリの記録装置の利用者がアクセスできない領域に保存しておき、必要に応じて、フラッシュメモリからアプリケーションを読み出し、RAMへ展開して実行する機能を有する記録装置を構成する。

【0013】

【発明の実施の形態】図1は、本発明が適用された記録装置120の構成図である。記録装置120は、タンパレジスタントモジュール121及びフラッシュメモリ140を有する。タンパレジスタントモジュール121は、外部から物理的な解析を行うことが困難なように構成された電子回路であり、ICカードなど、高度なセキュリティが要求される電子機器に使用される。内部バス123は、各回路間の情報を送受信するために使用される。フラッシュメモリインタフェース124は、フラッシュメモリ140とタンパレジスタントモジュール121とを接続するために使用される。

【0014】ホストインタフェース122は、記録装置120と記憶装置120と接続される外部機器とのアクセスコマンド110の送受信に使用される。CPU128は、記録装置120内の各回路を制御する。暗号処理回路126は、記録装置120内で暗号処理を行うためにCPU128によって使用される。RAM129は、データを一時的な記録するために使用されるワークRAMである。ROM130には、CPU128が恒久的に利用するプログラム及びデータが記録される。NVメモリ125は、小容量で書き込み回数が少ない不揮発性メモリである。NVメモリ125は、外部から解析されると危険な情報が記録される。NVメモリ125としては、例えば、EEPROMなどがある。NVメモリ125には、以下の情報及びプログラムが格納される。

【0015】秘密情報Km151には、タンパレジスタントモジュール121がフラッシュメモリ140へデータを読み書きする際に、データを暗号化、復号化するために使用する鍵の情報などが含まれる。Km対応暗号処理プログラム152は、秘密情報Km151を利用して暗号処理を行うアプリケーションである。

【0016】秘密情報Ko153には、サービスプロバイダ100のサーバ180と携帯端末103が、後述する公衆回線108に暗号化された通信経路を確立するために使用される証明書、鍵の情報などが含まれる。Ko対応暗号処理プログラム152は、秘密情報Ko153を利用して暗号処理を行うアプリケーションである。

【0017】秘密情報Ki155には、サービスプロバイダ100のサーバ180内の配信アプリケーション181と記録装置120が、後述する暗号化内部通信経路109を確立するために使用される記録装置証明書、鍵の

情報などが含まれる。Ki対応暗号処理プログラム156は、秘密情報Ki155を利用して暗号処理を行うアプリケーションである。

【0018】秘密情報Ki157には、CPU128が実行するアプリケーションが暗号処理を行う際に必要な証明書、鍵の情報などが含まれる。Ki対応暗号処理プログラム158は、秘密情報Ki157を利用して暗号処理を行うアプリケーションである。尚、Ki157は、アプリケーションによって独自の目的で使用される場合がある。Ki157は、アプリケーションごとに複数存在する場合もある。

【0019】NVメモリ125は、データエリア160を有する。データエリア160には、記録装置120を使用する者の個人的な情報、例えば、電話帳、スケジュール、クレジットカード情報、電子マネー、個人認証情報などが格納される。

【0020】これらの重要個人情報(鍵情報等)は、フラッシュメモリ140に格納することも考えられるが、悪意のものがカードを破壊して、読み出す可能性があるので、外部からの読み出しが困難なタンパレジスタントモジュール121のNVメモリ125に格納する。

【0021】アプリケーションRAM127は、CPU128がアプリケーション実行時にフラッシュメモリ140から読み出した暗号化されたアプリケーション144の暗号を復号して実行するために使用される。

【0022】フラッシュメモリ140は、一括消去書き込み可能な不揮発性メモリであり、例えば、記憶容量が大きい多値フラッシュメモリなどのフラッシュメモリチップが考えられる。フラッシュメモリ140は、ユーザアクセス禁止領域142及びユーザアクセス許可領域141を有する。ユーザアクセス禁止領域142に格納されたデータは、タンパレジスタントモジュール121内のCPU128のみによって消去及び書き込まれる。ユーザアクセス禁止領域142には、記録装置120が実行する暗号化されたアプリケーション144、記録装置120のファームウェア等の重要情報143等ユーザーによって操作されると困る情報が保存される。尚、このデータには、外部から改ざん不可能なように電子署名が付加される場合もある。ユーザアクセス許可領域141は、記憶装置120に接続される外部装置から自由にアクセスすることが可能な領域であり、コンテンツ402、暗号化されたプログラム、その他特に外部に見られても問題のないデータが保存される。

【0023】CPU128が使用する多種多様なアプリケーションプログラムは、フラッシュメモリ140にあらかじめ暗号化されて格納される。暗号化されたアプリケーションプログラム144は、使用される前に、タンパレジスタントモジュール121に供給される。その際に、CPU128は、Km151及びKm対応暗号処理プログラム152を用いて、アプリケーションプログラムを

復号化して、アプリケーション RAM127にロードする。ロードが完了すると、アプリケーションプログラムは実行可能となる。一方、音声、画像等のコンテンツ402は、フラッシュメモリ140に格納される。この際、CPU128は、アクセスコマンド110に応じてデータの格納先を自動的に解析する。解析手段の詳細は後述する。

【0024】図2は、本発明が適用された記憶装置120の実施形態を使用したシステムの構成図である。携帯端末103は、記録装置120と接続され、記録装置120を利用してサービスプロバイダ100と通信を行う機能を有する。携帯端末103は、表示画面104、スピーカ105、マイク106及びCCDカメラ107を有する。

【0025】サービスプロバイダ100は、記録装置120に対して、コンテンツ配信などを行うサーバ180を有する。サーバ180は、配信アプリケーション181、配信するコンテンツ182を有する。

【0026】サービスプロバイダ100と携帯端末103の間では、データの漏洩を防ぐために、公衆回線108上に、暗号化された通信経路を確立することが可能である。さらに、携帯端末103に接続された記録装置120は、サービスプロバイダ100との間に確立された暗号化された通信経路内で、さらに暗号化された内部通信経路109を確立することも可能である。図では、内部通信経路109は携帯端末103にのみ示されているが、実際は、公衆回線108上にも経路が確保されている。詳細は後述する。

【0027】サービスプロバイダ100、携帯端末103及び記録装置120を用いた本システムでは、サービスプロバイダ100と記録装置120がデータを送受信する際は、データは、サービスプロバイダ100と携帯端末103との間、すなわち公衆回線108上で2重に暗号化され、携帯端末103と記録装置120の間では1重に暗号化される。携帯端末103等で利用される暗号処理方式によっては、サービスプロバイダ100と携帯端末103間では、データはn+m重に暗号化され、携帯端末103と記録装置120間では、m重に暗号化される場合もある。尚、記録装置120を接続する機器は携帯端末103に限定されないし、公衆回線108は、有線回線でも無線回線でもよい。有線回線としては、光ケーブル等が考えられる。

【0028】図3は、携帯端末103の構成図である。CPU201は、携帯端末103の各回路を制御する。RAM202には、CPU201が利用するデータが一時的に保存される。ROM203には、CPU201が恒久的に利用する書き換えを行わないデータが記録される。携帯端末制御回路204は、携帯端末103と外部機器との情報の送受信などの処理を行う。入出力インタフェース205は、携帯端末103を利用する者のキー

入力、画面表示などの処理を行う。記録装置インタフェース207は、記録装置120との間で情報の送受信を行う。デコード回路206は、記録装置120から読み出した情報を、音声や映像などに復号する。バス208は、回路間における情報の送受信に使用される。

【0029】図4は、デコード回路206の構成を示す図である。デコード回路206は、記録装置120から読み出したデータを復号してから再生するため、復号されたデータを外部からアクセスできないようにする必要がある。このため、デコード回路206は、タンパレジスタントモジュールになっている。制御回路301は、デコード回路206内の各回路を制御する。RAM302には、復号した情報などが一時的に記録される。ROM303には、制御回路のプログラムなど恒久的に利用する情報で機密性が低いものが記録される。不揮発性メモリ306には、デコード回路206の証明書、記録装置120から取り出した暗号化されたデータを復号化するために必要な鍵など、機密性が高い情報が記録される。インタフェース307は、外部回路との接続に使用されるインタフェースである。バス308は、各回路間の情報の送受信に使用される。

【0030】図5は、本発明が適用された記録装置120が用いられるシステムにおける通信方式の一例を示す図である。記録装置120と携帯端末103との間の情報の送受信は、アクセスコマンド110でおこなわれる。アクセスコマンド110は、階層化されたアクセスコマンド（以下、「階層化コマンド」と称する）405で定義される。物理アクセスコマンド408は、記録装置120とのデータの入出力など基本的なコマンドである。論理アクセスコマンド409は、物理アクセスコマンド408のデータとして送受信される。記録装置120及び携帯端末103は、物理アクセスコマンド408を解析し、データ領域から論理アクセスコマンド409を取り出して実行する。このようなコマンド構成にすることで、携帯端末103と記録装置120との間での基本的なコマンドに変更を加えることなく、容易にコマンドを拡張することが出来る。

【0031】ライセンス401は、暗号化コンテンツ402を復号化するための鍵を含む情報である。暗号化コンテンツ402は、ライセンス401によって暗号化されたコンテンツである。ライセンス配信404の矢印は、サービスプロバイダ100からネットワーク403、携帯端末103を介して記録装置120のタンパレジスタントモジュール121へライセンス401を配信する場合を示している。コンテンツ配信407の矢印は、サービスプロバイダ100から記録装置120へコンテンツ402を配信する場合を示している。サービスプロバイダ100と携帯端末103との間では、ライセンス401及びコンテンツ402は、階層化コマンド406を利用して配信される。携帯端末103と記録装置

120の間では、ライセンス401は階層化コマンド405を利用して配信され、タンパレジスタントモジュール121へ格納される。コンテンツ402は、携帯端末103と記録装置120の間では、物理アクセスコマンド408のみを利用して記録装置120内のフラッシュメモリ140へ配信される。

【0032】図19は、物理アクセスコマンド408及び論理アクセスコマンド409の構成例を示す図である。物理アクセスコマンド408は、コマンドコード1801、長さ1802及びデータエリア1803から構成されている。コマンドコード1801は、コマンドタイプ1810、属性1811及びセキュリティレベル1812から構成されている。コマンドタイプ1810と属性1811には、図19の表に示すような対応関係の情報が格納されている。属性1811とは、例えばデータが個人情報、鍵情報などであるか、他の一般的な情報であるか等を示すタグなどである。以下このような属性を表すデータを、属性データという。セキュリティレベル1812には、コマンドによって送信されるデータの機密性のレベルを示す情報が格納される。機密性のレベルは、本実施形態の場合、3段階に分かれている。セキュリティレベルは、送信されるデータの性質に応じて、アクセスコマンド110を発行する装置によって発行時にアクセスコマンド110に付加される。

【0033】長さ1802には、データエリア1803の長さを表す情報が格納される。データエリア1803には、通常のデータの他に、論理アクセスコマンド409も含まれる。

【0034】論理アクセスコマンド409は、コマンドコード1804、長さ1805及びデータ1806で構成される。コマンドコード1804は、物理アクセスコマンド408のコマンドコード1801と同一である。長さ1805には、データ1806に格納されるデータの長さを示す情報が格納される。データ1806には、実際のデータが格納される。

【0035】階層化コマンド406とそれを構成する物理アクセスコマンド410と論理アクセスコマンド411も階層化コマンド405と同様な構成になっている。階層化コマンド406は、携帯端末103とサーバ180がネットワーク403を介して情報を送受信する場合に利用される。尚、階層化コマンド405と階層化コマンド406の具体的なコマンドコードなどは異なってもかまわない。

【0036】図20は、記録装置120が行うコマンド受信した階層化コマンドの振り分け処理を示すフロー図である。記録装置120は、物理アクセスコマンド408を受信する(1901)。記録装置120内のCPU128は、物理アクセスコマンド408のコマンドコード1801をチェックする(1902)。論理アクセスコマンド409が存在すれば、CPU128は、論理アクセ

スコマンドの解析を実行する(1904)。CPU128は、論理アクセスコマンド409を処理する(1905)。物理アクセスコマンド408に論理アクセスコマンド409が含まれていない場合は、CPU128は、物理アクセスコマンド処理を実行する(1903)。コマンドの処理が終了すると、CPU128は、データ選別処理を行い、秘匿性の高いデータと低いデータを識別してそれぞれのデータに適した領域に記録を行う(1906)。

【0037】図21は、CPU128が実行するデータ選別処理1906を示したフロー図である。CPU128は、携帯端末103より送信されてきた物理アクセスコマンド408又は論理アクセスコマンド409のコマンドタイプ1810がWRITEコマンドかどうか調べ(2002)、WRITEコマンド以外なら処理を終了する(2009)。コマンドタイプ1810がWRITEコマンドなら、CPU128は、データエリア内のデータを調べ、属性1811に属性データが存在するか調べる(2003)。属性1811に属性データが存在しないなら、CPU128は、コマンドコードのセキュリティレベル1812をチェックする(2004)。CPU128は、セキュリティレベルが1なら、NVメモリ125の空き容量を調べ(2005)、空き容量が十分あるなら、データをNVメモリ125へ格納する(2006)。空き容量が十分ないなら、CPU128は、データを暗号化して(2007)、データをフラッシュメモリ140へ書き込む(2008)。セキュリティレベルが2なら、CPU128は、データを暗号化して(2007)、データをフラッシュメモリ140へ書き込む(2008)。セキュリティレベルが3なら、CPU128は、データをフラッシュメモリ140へ書き込む(2008)。ステップ2003で属性1811に属性データが存在すると判断したら、CPU128は、属性データの内容を判断する(2010)。属性データによって、アクセスコマンドによって送られてきたデータが小容量の機密データであると判断されるなら、CPU128は、NVメモリ125の空き容量を調べ(2011)、空き容量があるなら、データをNVメモリ125へ格納する(2012)。空き容量が十分無いなら、CPU128は、データを暗号化して(2013)、データをフラッシュメモリ140へ格納する(2014)。大容量の機密データと判断されると、CPU128は、データを暗号化して(2013)、データをフラッシュメモリ140へ格納する(2014)。暗号化の必要がないなら、CPU128は、データをそのままフラッシュメモリ140へ格納する(2014)。

【0038】図6は、公衆回線108における暗号化された通信経路確立処理510及び暗号化内部通信経路確立処理520を示すフロー図である。これらの手順をまとめて暗号化通信経路確立処理500と称する。

【0039】公衆回線108における暗号化された通信経路確立処理510を説明する。携帯端末103は、秘密情報Ko153を記録装置120から取り出す(502)。携帯端末103は、秘密情報Ko153を暗号化してサービスプロバイダ100へ送信する(503)。暗号化された秘密情報Ko153を受信したサービスプロバイダ100のサーバ180は、秘密情報Ko153を復号化して取り出す(504)。その後の通信においては、サーバ180と携帯端末103が秘密情報Ko153で情報を暗号化して送受信する。これによって、暗号化された通信経路が確立される(506)。

【0040】暗号化内部通信経路確立処理520を説明する。記録装置120は、秘密情報Ki155を暗号化し、携帯端末103及びサービスプロバイダ100間で確立されている暗号化された通信経路を用いて、暗号化された秘密情報Ki155をサービスプロバイダ100へ送信する(509)。暗号化された秘密情報Ki155を受信したサービスプロバイダ100のサーバ180は、秘密情報Ki155を復号化して取り出す(510)。その後、サーバ180と記録装置120が秘密情報Ki155で情報を暗号化して情報を送受信する(511)。これによって、暗号化内部通信経路が確立される(512)。

【0041】図7は、携帯端末103と記録装置120、サーバ180の間での著作権保護の基本的な流れを示す図である。この図では、サーバ180から記録装置120へ著作権を保護したいコンテンツ402を送信する場合について示している。各送信手順の表記は、図22に示す表記法規定2101に従う。尚、図7においてはKs1はサーバ180が乱数などを使用して生成する。Ks2は記録装置120の暗号処理回路126が乱数などを使用して生成する。利用者が携帯端末103を操作して、コンテンツ取得を記録装置120へ指示すると、記録装置120がコンテンツ要求601を携帯端末103を通してコンテンツ402を保持しているサーバ180へ発行する。これによって記録装置120は、取得したいコンテンツ402に対応したContent IDと記録装置120が正当な機器であることを証明する証明書C(Ka, KPmc || Imc)をサーバ180へ送信する(602)。サーバ180が、コンテンツIDと証明書を受信すると、証明書をチェックする。証明書が正規のものであれば、記録装置120へセッション鍵E(KPmc, Ks1)を送信する(603)。セッション鍵Ks1を記録装置120が受信すると、セッション鍵Ks2を含めた様々な情報をE(Ks1, KPm1 || Ks2 || CRLUpdate)としてサーバ180へ送信する(604)。これを受信したサーバ180はライセンス401を含む様々な情報をE(Ks2, CRL || E(KPm1, TransactionID || Acn || Kc || Acp))として記録装置120へ送信する(605)。続いて、サーバ180は、コンテンツ402を記録装置120へE(Kc, C

ontent)として送信する(606)。以下で説明する情報の送受信はここで述べた方式を利用する。

【0042】図8は、記録装置120、携帯端末103及びサーバ180それぞれのソフトウェアの階層構造を表している。以下の記載では、サービスプロバイダ100の記載を省略する。記録装置120では、暗号化計算部702の上にアプリケーション701が構成されている。アプリケーション701が、暗号化計算部702を利用して暗号処理などを行う。ソフトウェアはタンパレジスタントモジュール121に構成される。アプリケーション701は、記録装置120内のデータ処理から暗号化通信など記録装置が提供するサービスに応じたアプリケーション701が搭載される。暗号化計算部702は、暗号に関する計算処理を行う。暗号化処理部702は、アプリケーション701だけでなく、携帯端末103の暗号化通信処理部704にも利用される。

【0043】携帯端末103では、通信基本処理部705の上に、暗号化通信処理部704が構成され、さらにその上に、携帯端末アプリケーション703が構成される。通信基本処理部705は、携帯端末103の通信の基本的な処理、例えば、通信路符号化、通信速度の変更、データの送受信などの処理を行う。暗号化通信処理部704は、送受信するデータをサーバ180との間で取り決めた暗号化方式を用いて暗号処理する。暗号化通信に必要なデータの準備や、暗号計算などの処理は、記録装置120の暗号化計算部702を利用して行われる。携帯端末アプリケーション703は、メニュー表示、電子メール機能など、利用者が携帯端末103で利用するさまざまなアプリケーションである。サーバ180では、ソフトウェアは、基本通信処理部706、暗号化通信処理部707及びサーバアプリケーション708から構成される。基本通信処理部706及び暗号化通信処理部707は、携帯端末103の基本通信処理部704及び暗号化通信処理部705と同様の動作をする。ただし、暗号化通信処理部707は、暗号化に関する処理を行うときに、記録装置120を利用しなくてもよい。サーバアプリケーション708は、携帯端末103に配信するコンテンツ402の管理、利用者の管理など、一般的にサーバとして機能するために必要なアプリケーションである。

【0044】記録装置120が、携帯端末103を介してサーバ180からコンテンツ402を取得する場合について説明する。図9に示すように、携帯端末103及びサーバ180の暗号化通信処理部704、707が、基本通信処理部705、706を介して暗号化通信経路801を構成する(これは、暗号化された内部通信経路109に相当する)。暗号化通信処理部704は、記録装置120内の暗号化計算部702を利用して暗号化に関する計算を行うと共に、利用者に関する情報をサーバ180へ送信し、暗号化通信経路801で暗号化及び復

号化に利用する一時的な鍵情報などを記録する。

【0045】暗号化通信経路701が構成されると、図10に示すように、記録装置120、携帯端末103及びサーバ180の各アプリケーションが起動する。記録装置120のアプリケーション701が、携帯端末103と暗号化通信経路701を介して、サーバアプリケーション708から取得したいコンテンツ402に対応するライセンス401を取得し、記憶装置120のタンパレジスタントモジュール121へ保存する。

【0046】ライセンス401の取得が終了すると、図11に示すように、記録装置120のアプリケーション701が、携帯端末103と暗号化通信経路801を介して、サーバアプリケーション708から暗号化コンテンツ401を取得し、携帯端末103のフラッシュメモリ140へ保存する。尚、コンテンツ401がすでに暗号化されているため、この手順では、単にサーバ180から受信したデータを記録装置120へ保存するだけでよいので、物理アクセスコマンド408のみを用いて処理を行う。論理アクセスコマンド409を利用してもかまわない。

【0047】図12は、図8～図11における通信の処理手順を示したフロー図である。アプリケーション起動処理が実行される(1100)。携帯端末103は、携帯端末103が行う通信に必要な処理をするアプリケーションを記録装置120内から選択する(1101)。CPU128は、携帯端末103に選択されたフラッシュメモリ140に格納されているアプリケーションが暗号化されているかチェックする(1103)。暗号化されている場合は、CPU128は、秘密情報Km151を用いてアプリケーションを復号化して、アプリケーションRAM127に格納する(1104)。暗号化されていない場合は、CPU128は、そのままフラッシュメモリ140より読み出して、アプリケーションRAM127に実行可能な状態で格納する。CPU128は、アプリケーションを実行する(1106)。

【0048】アプリケーションが起動すると、携帯端末103及び記憶装置120は、暗号化通信経路確立処理500を実行して、サーバ180と通信経路を確立する。

【0049】記憶装置120とサーバ180との間で送受信処理1120が実行される。このとき、暗号化通信経路確立処理500の暗号化内部通信経路確立処理520で使用した秘密情報Ki155を利用してサーバ180と記録装置120が互いのデータを暗号化し、携帯端末103を中継して送受信を行う(1107～1118)。携帯端末103は、記憶装置120が送受信しているデータを見ることはできない。携帯端末103は、記録装置120の送信終了を示すデータだけを識別することができるため、該当するデータが記憶装置120から送信されてくると、送受信処理1120を終了する。

【0050】携帯端末103は、送受信処理1120を終了するため、終了処理1130を実行する。具体的には、携帯端末103は、処理終了通知を記録装置120とサーバ180へ送信する(1132、1135)ことでサーバ180に通信経路を破棄させ(1133)、記録装置120にアプリケーションを終了させる(1136)。

【0051】図13は、サーバ180から記録装置120へ、携帯端末103を経由してライセンス401をダウンロードする場合の具体的なコマンドのやり取りを示した図である。説明は図12と対応付けて行う。

【0052】アプリケーション起動処理1100では、以下のコマンドがやり取りされる。OPEN_CHANNEL 1201は、携帯端末103から記録装置120へ、両者間で仮想の通信経路を構成するために発行されるコマンドである。記録装置120は、仮想通信経路の番号を返す。以後の通信は、仮想通信経路番号を利用して行われる。

【0053】OPEN_FILE 1202は、携帯端末103が記録装置120内のライセンス401を保存するファイルを指定するコマンドである。記録装置120は、指定されたファイルの割り当て番号を返す。以後の処理はこのファイル割り当て番号を利用して行われる。VERIFY 1203は、携帯端末103が記録装置120内のアプリケーションを起動するための認証コードを発行するコマンドである。記録装置120が認証コードが正規のものであると認証すると、記録装置120内部のアプリケーションが起動され、OPEN_FILE 1202で指定したファイルがアクセスできるようになる。

【0054】公衆回線における暗号化された通信経路確立処理510が行われる。暗号化内部通信経路確立処理520では、以下のコマンドがやり取りされる。SEND_CERT 1205は、携帯端末103が、記録装置120へ正当な記録装置120であることを証明する証明書の送信を要求するコマンドである。記録装置120は、証明書を携帯端末103へ送信する。

【0055】OPEN 1206は、携帯端末103が、記録装置120から読み出した証明書とContentIDをサーバ180へ送信するコマンドである。証明書をサーバ180が認証すると、サーバ180は、セッション鍵Ks1を生成して携帯端末103へ送信する。SET_SESSION_KEY 1207は、携帯端末103が、サーバ180から受信したセッション鍵Ks1を記録装置120へ送信するコマンドである。尚 SEND_CERT 1205、OPEN 1206及びSET_SESSION_KEY 1207のコマンドは、図7のコンテンツ要求601とセッション鍵Ks1送信602に対応する。

【0056】送受信処理1120では、以下のコマンドがやり取りされる。ESTABLISH_WRITE_SESSION 1208は、記録装置120がセッション鍵Ks2を生成し、そ

れをKs1で暗号化したものを携帯端末103へ送信するコマンドである。

【0057】ESTABLISH_WRITE_SESSION 1209は、携帯端末103が、記録装置120から受信したKs1で暗号化されたKs2をサーバ180へ送信するコマンドである。暗号化されたKs2を受信したサーバ180は、Ks1で暗号化Ks2を復号し、Ks2でライセンス401を暗号化して、携帯端末103へ暗号化されたライセンス401を送信する。

【0058】SET_LICENSE 1210は、携帯端末103が、ライセンス401を記録装置120へ送信するコマンドである。

【0059】WRITE_LICENSE 1211は、携帯端末103が、記録装置120に、ライセンス401をKs2で復号化し、タンパレジスタントモジュール121のNVメモリ125へライセンス格納領域を作成しそこに格納させるために発行するコマンドである。尚、ESTABLISH_WRITE_SESSION 1208、1209、SET_LICENSE 1210及びWRITE_LICENSE 1211は、図7のKs1でセッション鍵Ks2送信603及びライセンス送信604に対応する。

【0060】終了処理1130では、以下のコマンドがやり取りされる。CLOSE 1212は、携帯端末103が、サーバ180へライセンス取得処理が終了したことを知らせるコマンドである。CLOSE 1212をサーバ180が受信すると、サーバ180は、携帯端末103とサーバ180の間の暗号化通信経路801を破棄する。CLOSE_FILE 1213は、携帯端末103が、記録装置120のファイルを閉じるために発行するコマンドである。CLOSE_CHANNEL 1214は、携帯端末103が記録装置120との間で利用していた仮想通信経路を閉じて処理を終了するために発行するコマンドである。図14は、サーバ180から記録装置120へ携帯端末103を経由してコンテンツ402がダウンロードされる場合のコマンドのやり取りを示す図である。説明は図11と対応付けて行う。

【0061】公衆回線108における暗号化された通信経路確立処理510が行われる。送受信処理1120では、以下のコマンドがやり取りされる。OPEN 1301は、携帯端末103が、取得したいContentIDをサーバ180へ送信するコマンドである。ContentIDをサーバ180が受信すると、サーバ180は、暗号コンテンツ402を携帯端末103へ送信する。SET_BLOCKS_TRANSFERRED 1302は、携帯端末103が、サーバ180から受信した暗号化コンテンツ402のサイズを記録装置120へ送信するためのコマンドである。WRITE_BLOCK 1303は、携帯端末103が、サーバ180から受信した暗号化コンテンツ402を記録装置120内のフラッシュメモリ140上の任意のアドレスへ転送するためのコマンドである。アドレスの指定方法としては、フラ

ッシュメモリ140上にファイルシステムを設け、ContentIDを元に暗号化コンテンツ402に対応するファイルが作成され、ファイルシステムが定めたアドレスを指定する方法などが考えられる。暗号化コンテンツ402の容量が大きい場合は、SET_BLOCKS_TRANSFERRED 1302及びWRITE_BLOCK 1303が複数回発行される場合もある。

【0062】CLOSE 1304は、携帯端末103が、サーバ180へライセンス取得処理が終了したことを知らせるコマンドである。CLOSE 1304をサーバ180が受信すると、サーバ180は、携帯端末103とサーバ180の間の暗号化通信経路を破棄する。尚、図14の手順は、図7のコンテンツ送信605に対応する。

【0063】図15は、記録装置120内の暗号化コンテンツ402を携帯端末103内のデコーダ回路206が再生する場合の概念図である。デコーダ回路206は、携帯端末103以外の機器に搭載されて使用されることも可能である。記録装置120も、携帯端末103以外の機器と接続されることも可能である。具体例としては、MP3プレーヤ、ステレオ、デジタル映像再生機などが考えられる。デコーダ回路206は、記録装置120のタンパレジスタントモジュール121から、再生したい暗号化コンテンツ402のライセンス401を取り出す。デコーダ回路206は、フラッシュメモリ140から暗号化コンテンツ402を取り出し、暗号化コンテンツ402をライセンス401で復号化してから再生する。ライセンス送信1402は、階層化コマンド405を用いて行われる。コンテンツ送信1403は、物理アクセスコマンド408を用いて行われる。尚、それぞれの送信時のコマンドの構成に付いてはこの限りではない。

【0064】図16は、図15における通信の詳細を示したフロー図である。アプリケーション起動処理(1100)から、アプリケーションを実行する(1106)までの処理は、図11で説明したフローと同一であるので、説明を省略する。

【0065】アプリケーションが起動すると、暗号化内部通信経路確立処理520が実行され、デコーダ回路206と記録装置120との通信経路が確立される。この場合、デコーダ回路206専用の秘密情報K1157を用いて通信経路が確立される。

【0066】送受信処理1500が実行され、実際に記録装置120とデコーダ回路206の間でデータの送受信が行われる。このとき、暗号化内部通信経路確立処理520で使用した秘密情報K1157を利用してデコーダ回路206と記録装置120が互いのデータを暗号化し送受信を行う(1501~1508)。送受信処理1500の最中は、携帯端末103の制御は、デコーダ回路206によって行われている。送受信が終了すると、デコーダ回路206は、携帯端末のCPU201に終了割

り込みを知らせるコマンドを送付する。終了割り込みのコマンドを受けたCPU201は、終了処理1510を開始する。具体的には、携帯端末103のCPU201は、処理終了通知を記録装置120に送信して(1512)、アプリケーションを終了させる(1513)。

【0067】図17は、デコーダ回路206が、ライセンス401を取得する際の記録装置120との間での手順のコマンドを示したものである。説明は図16と対応付けて行う。尚、図17においては表記法規定2101のデータの所在で秘密情報K1155と記載されているところは、すべて秘密情報K1に置き換わる。また、Ks5は記録装置120の暗号処理回路126が乱数などを使用して生成し、Ks6はデコーダ回路206の暗号処理回路304が乱数などを使用して生成する。

【0068】アプリケーション起動処理1100では、以下のコマンドがやり取りされる。OPEN_CHANNEL 1600は、デコーダ回路206が、記憶装置120との間で仮想の通信経路を確立するために、携帯端末103の記録装置インタフェース207を介して記録装置120へ発行するコマンドである。OPEN_CHANNEL 1600コマンドを受け取った記録装置120は、仮想通信経路の番号を返す。以後の通信は、この仮想通信経路番号を利用して行われる。

【0069】OPEN_FILE 1601は、デコーダ回路206が、記録装置120内のライセンス401が保存されているファイルを指定するためのコマンドである。OPEN_FILE 1601コマンドを受け取った記録装置120は、指定されたファイルの割り当て番号を返す。以後の処理はファイル割り当て番号を利用して行われる。

【0070】VERIFY 1602は、デコーダ回路206が、記録装置120内のアプリケーションを起動するための認証コードを発行するコマンドである。記録装置120が認証コードが正規のものであると認証すると、記録装置120内部のアプリケーションが起動され、OPEN_FILE 1601で指定したファイルがアクセスできるようになる。

【0071】秘密情報K1157が使用される暗号化内部通信経路確立処理520では、以下のコマンドがやり取りされる。

【0072】VERIFY_CERT 1604は、デコーダ回路206が、証明書を記録装置120へ送信するコマンドである。VERIFY_CERT 1604コマンドを受信した記録装置120は、証明書を認証する。

【0073】SEND_SESSION_KEY 1605は、記録装置120が、デコーダ回路206へ暗号処理回路126で生成したセッション鍵Ks5を送信するコマンドである。ESTABLISH_PLAY_SESSION 1606は、Ks5を受け取ったデコーダ回路206が、暗号処理回路304で生成したセッション鍵Ks6を生成し、Ks6をKs5で暗号化して記録装置120へ送信するコマンドである。

【0074】送受信処理1500では、以下のコマンドがやり取りされる。READ_LICENSE1607は、デコーダ回路206が、記録装置120へ読み出すライセンス401の準備を指示するコマンドである。SEND_PLAY_LICENSE1608は、デコーダ回路206が、記録装置120からライセンス401を読み出すコマンドである。

【0075】終了処理1510では、以下のコマンドがやり取りされる。CLOSE_FILE1609は、デコーダ回路206が、記録装置120のファイルを閉じるために発行するコマンドである。CLOSE_CHANNEL1610は、携帯端末103が、記録装置120との間で利用していた仮想通信経路を閉じて処理を終了するために発行するコマンドである。

【0076】図18は、ライセンス401の取得を終了したデコーダ回路206が、記録装置120から再生を行う暗号化コンテンツ402を読み出す処理を示した図である。尚、この手順に付いては、コンテンツ402がすでに暗号化されているため、単に記録装置120からデコーダ回路206へデータを読み出すだけでよいので、物理アクセスコマンド408のみを用いて処理を行う。論理アクセスコマンド409を利用してもかまわない。

【0077】図18の処理では、以下のコマンドがやり取りされる。SET_BLOCKLEN1704は、デコーダ回路206が、読み出す暗号化コンテンツ402のサイズを記録装置120へ送信するコマンドである。SENT_BLOCKS_TRANSFERRED1705は、デコーダ回路206が、記録装置120内の暗号化コンテンツ402を一度に読み出す量を指定するコマンドである。READ_BLOCK1706は、デコーダ回路206が、再生する暗号化コンテンツ402のアドレスを記録装置120へ指定して暗号化コンテンツ402を読み出し、再生を行うために発行するコマンドである。

【0078】このような構成とすることによって、安全にかつ大容量のデータを保存することが出来る。

【0079】

【発明の効果】本発明では、タンパレジスタントモジュール及び大容量フラッシュメモリを搭載する記憶装置で秘匿性の高いデータを暗号化して大容量フラッシュメモリへ保存するので、データの秘匿性は維持したまま、大容量の秘匿性の高いデータを保持することが可能な安価な記録装置を構成することが出来る。また、記録装置内部で暗号処理を行い、外部機器が暗号鍵や暗号化、復号化を行う必要がないため、外部機器の負担が軽くなる。

【0080】また、本発明では、タンパレジスタントモジュールにCPUを搭載し、これが外部より送信されてきたデータの秘匿性を様々な条件に応じて判定し、秘匿性の高い情報は、タンパレジスタントモジュール内の不揮発性メモリへ保存し、秘匿性の低い情報は外部のフラ

ッシュメモリへ保存するようにするので、すべてのデータを暗号化する場合に比べてデータ処理が高速で、しかもタンパレジスタントモジュール内の記録領域を有効利用することができる。

【0081】さらに、本発明では、タンパレジスタントモジュール内で実行するアプリケーションを暗号化して外部フラッシュメモリへ保存し、必要場合はそれらをフラッシュメモリから読み出し内部のRAMへ展開して実行できるようにすることで、様々なアプリケーションを記録装置に一度に搭載することが可能で、しかも規模の大きなアプリケーションを記録装置内で実行できる。

【図面の簡単な説明】

【図1】本発明を適用した記憶装置の実施形態を示す構成図である。

【図2】本発明を適用した記録装置を利用するシステムの構成を示す図である。

【図3】本発明を適用した記録装置が接続される携帯端末の構成図である。

【図4】携帯端末に搭載されたデコーダ回路の構成図である。

【図5】記録装置と携帯端末そしてサーバ間でのコマンド体系を示す図である。

【図6】暗号化通信経路確立処理のフロー図である。

【図7】携帯端末に接続された記録装置がサーバからコンテンツとライセンスを取得する処理手順を示したフロー図である。

【図8】本発明が適用された各機器のソフトウェアの構成を示す図である。

【図9】本発明における暗号化通信経路の確立を示す図である。

【図10】本発明におけるライセンスの移動を示す図である。

【図11】本発明におけるコンテンツの移動を示す図である。

【図12】本発明におけるダウンロード時の処理手順を示すフロー図である。

【図13】本発明におけるライセンス取得時のコマンドのやり取りを示すフロー図である。

【図14】本発明におけるコンテンツ取得時のコマンドのやり取りを示すフロー図である。

【図15】本発明のコンテンツ再生時の機器の構成を示す図である。

【図16】本発明における再生時の処理を示したフロー図である。

【図17】デコーダ回路のライセンス取得のコマンドのやり取りを示したフロー図である。

【図18】デコーダ回路のコンテンツ取得のコマンドのやり取りを示したフロー図である。

【図19】本発明におけるアクセスコマンドの構成を示す図である。

【図20】記録装置のコマンド解析の流れを示したフロー図である。

【図21】記録装置のデータ選別処理の手順を示したフロー図である。

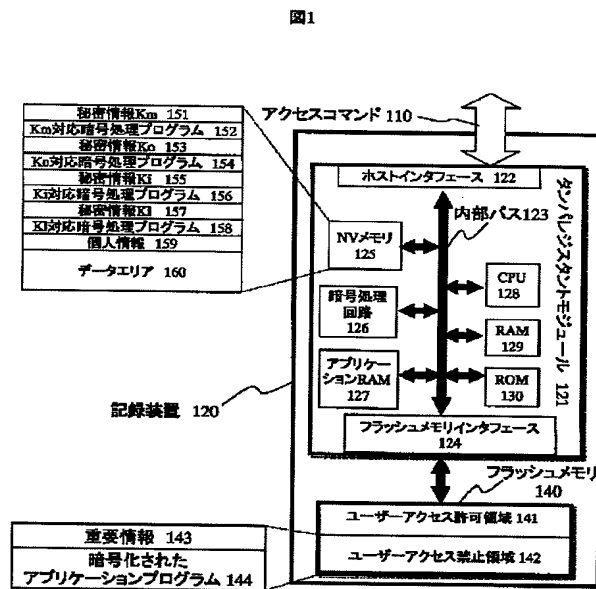
【図22】本発明で使用する表記法規定を示す図である。

【符号の説明】

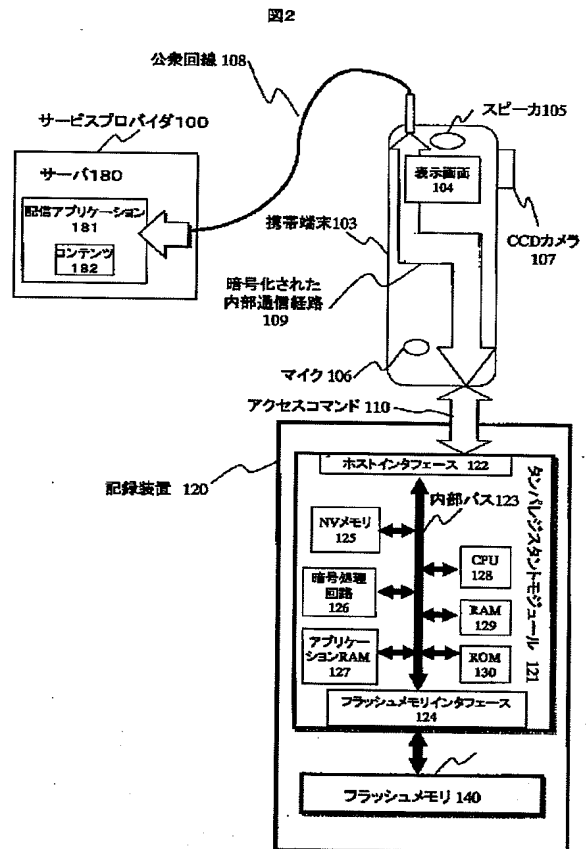
100…サービスプロバイダ、101…配信アプリケーション、103…携帯端末、108…公衆回線、109…暗号化内部通信経路、110…アクセスコマンド、120…記録装置、121…タンパレジスタントモジュール、125…NVメモリ、140…フラッシュメモリ、141…ユーザーアクセス許可領域、142…ユーザーアクセス許可領域、151…秘密情報Km、152…Km対応暗号処理プログラム、160…データエリア、206…

デコーダ回路、401…ライセンス、402…暗号化コンテンツ、403…ネットワーク、404…ライセンス配信、405、406…階層化コマンド、407…コンテンツ配信、408、410…物理アクセスコマンド、409、411…論理アクセスコマンド、500…暗号化通信経路確立処理、601…コンテンツ要求、604…ライセンス送信、605…コンテンツ送信、701…アプリケーション、702…暗号化計算部、703…携帯端末アプリケーション、801…暗号化通信経路、901…ライセンス配信、1001…暗号化コンテンツ配信、1100…アプリケーション起動処理、1120…送受信処理、1130…終了処理、1801…コマンドコード、1802…長さ、1803…データエリア、1811…属性、1812…セキュリティレベル。

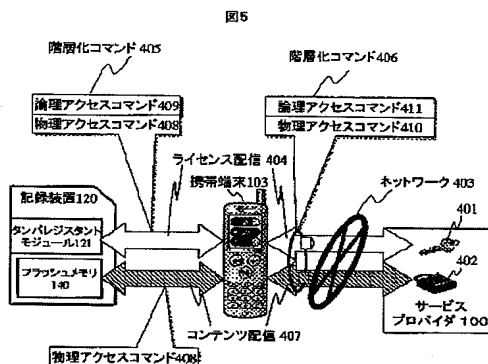
【図1】



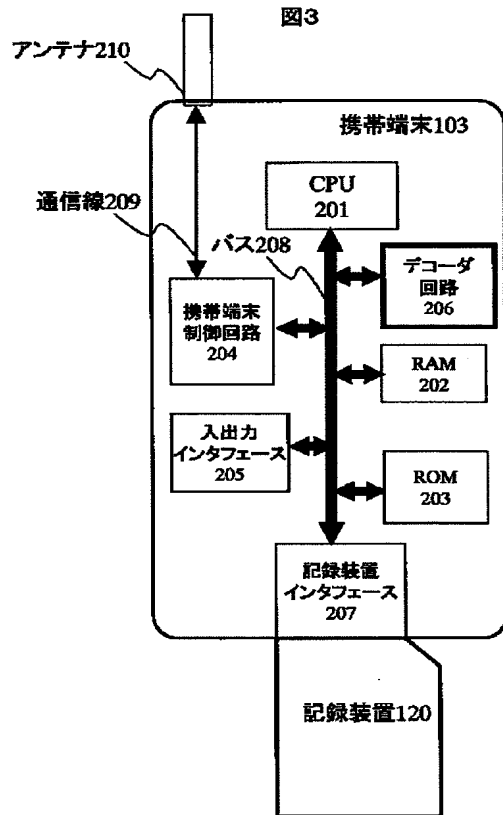
【図2】



【図5】

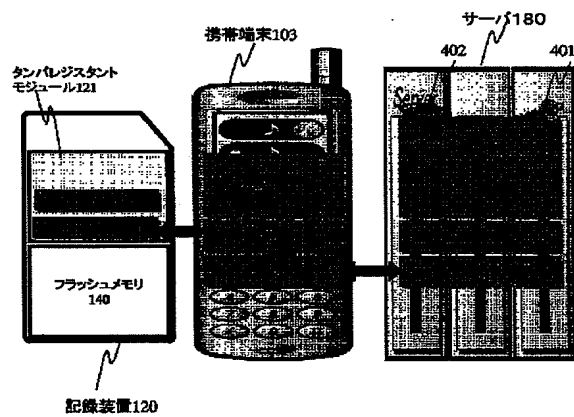


【図3】

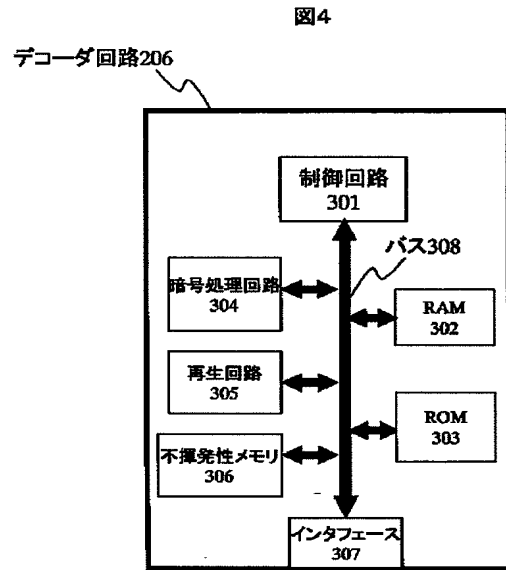


【図8】

図8

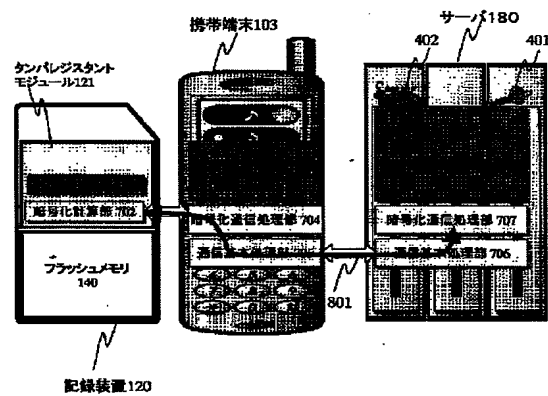


【図4】



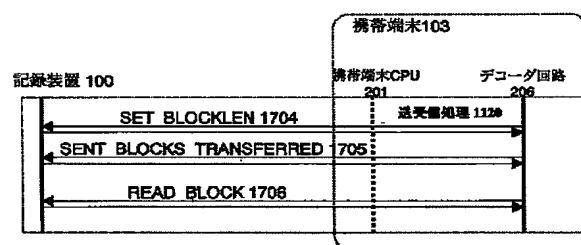
【図9】

図9



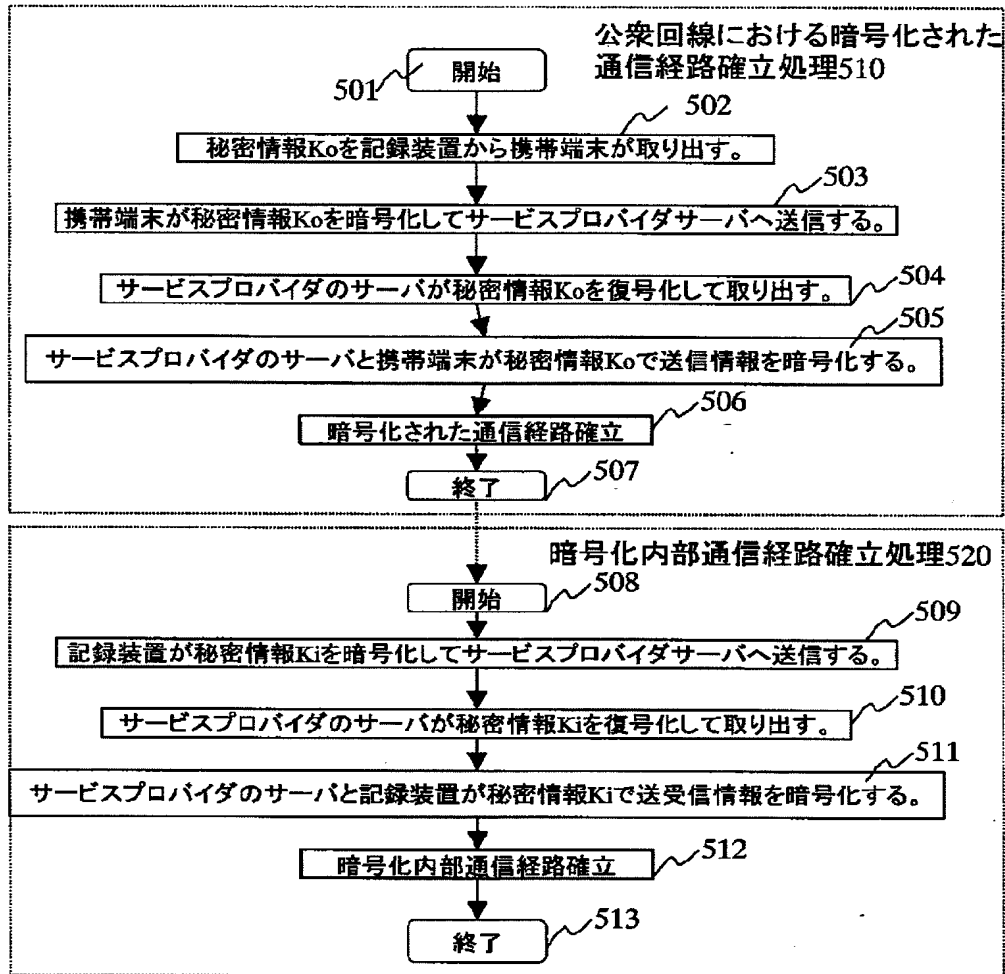
【図18】

図18



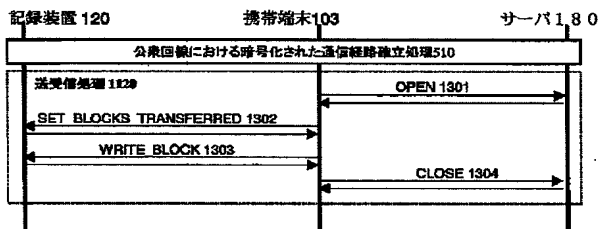
【図6】

図6 暗号化通信経路確立処理500



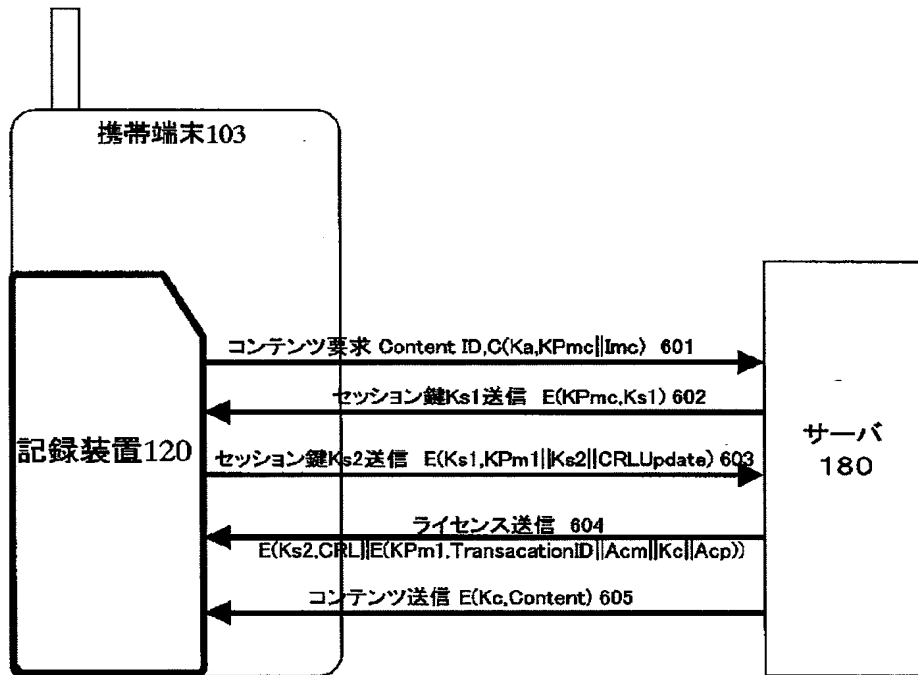
【図14】

図14



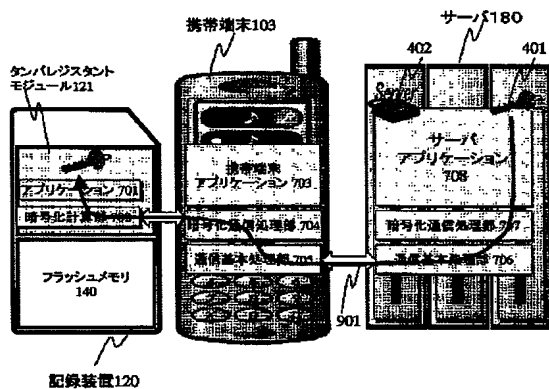
【図7】

図7



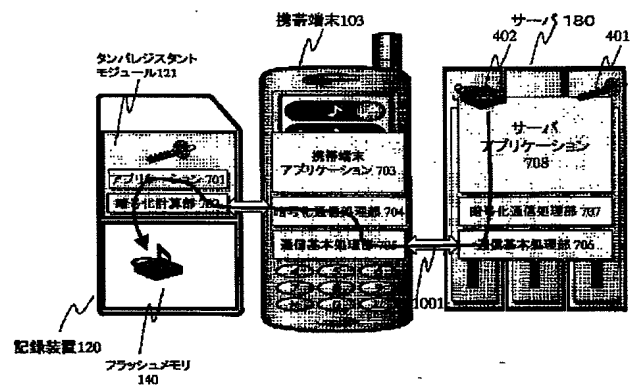
【図10】

図10



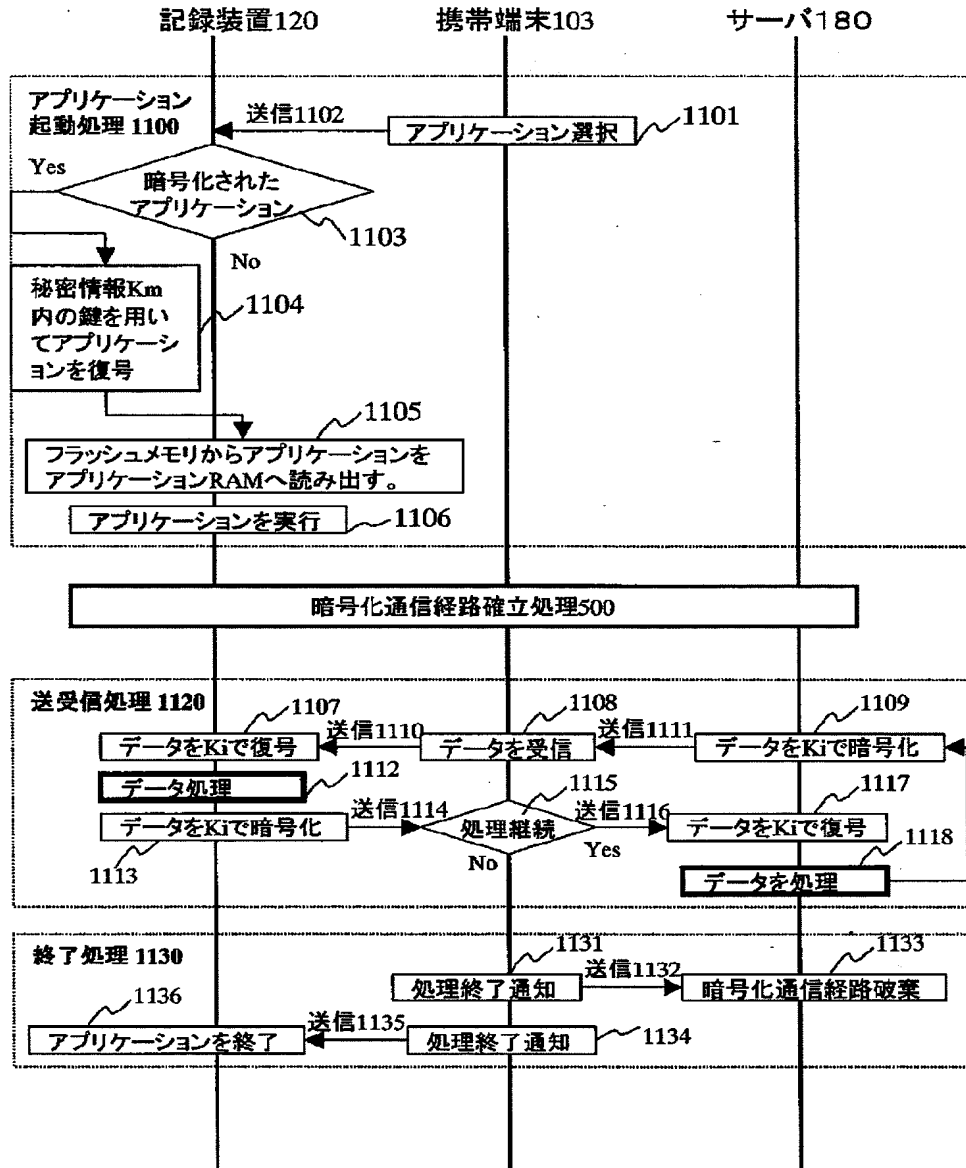
【図11】

図11



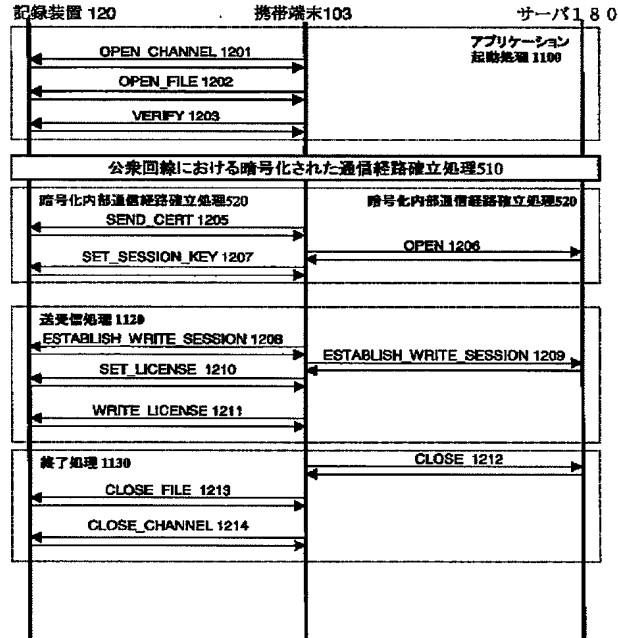
【図12】

図12



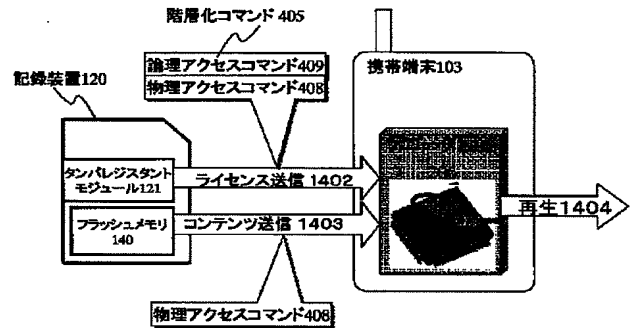
【図13】

図13



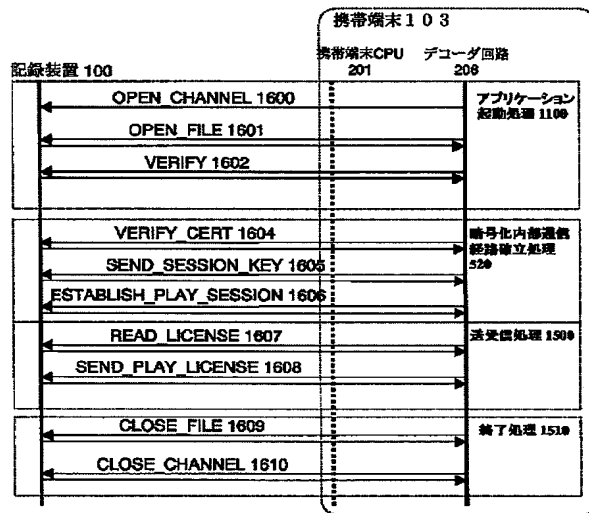
【図15】

図15



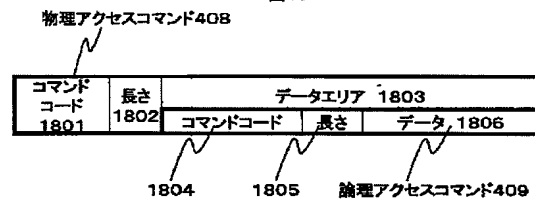
【図17】

図17



【図19】

図19



コマンドコード1801,1804

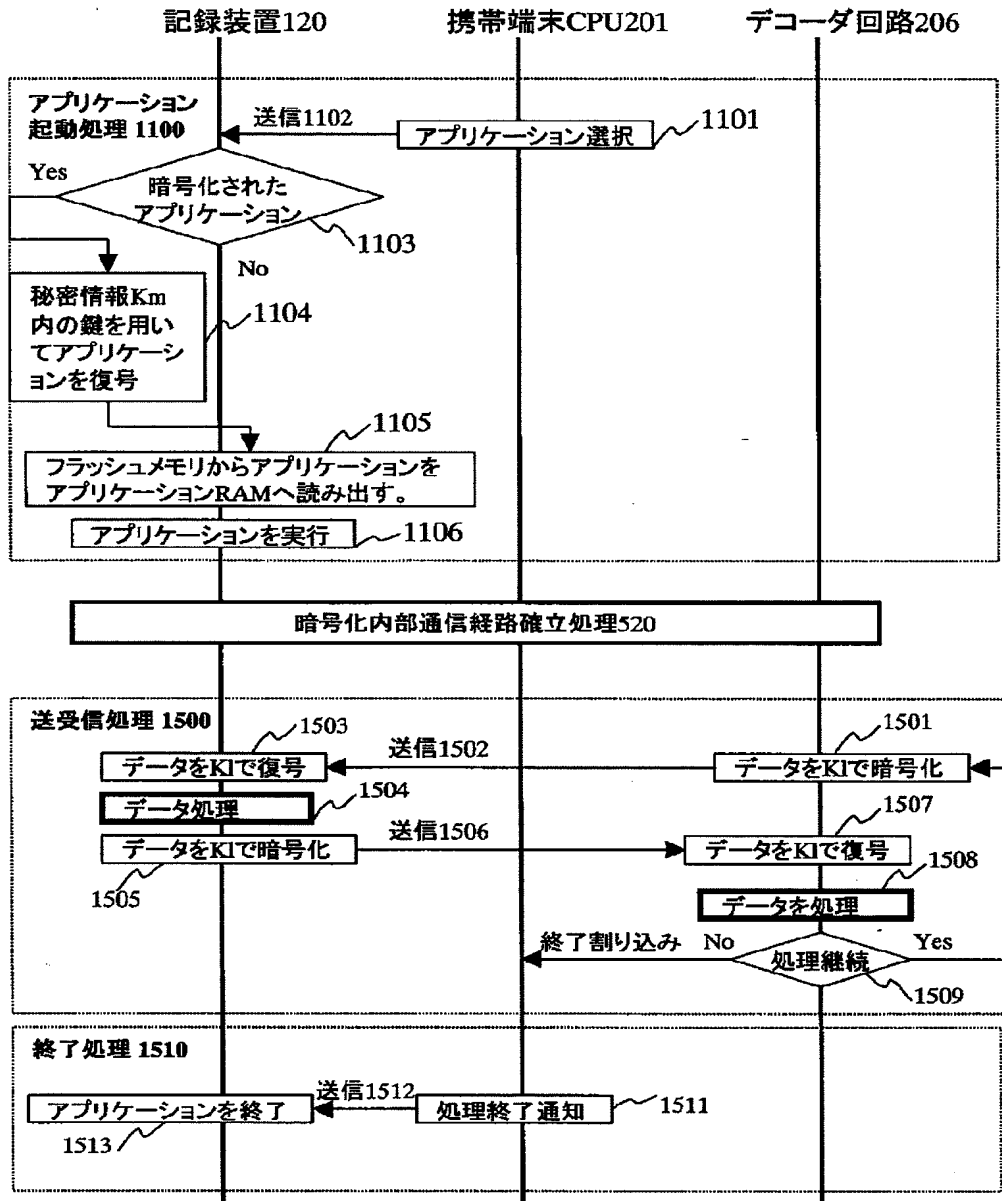
コマンドタイプ 1810	属性 1811	セキュリティレベル 1812
-----------------	------------	-------------------

コマンドタイプ1810	属性1811
READ	格納アドレス、データ長
WRITE	格納アドレス、データ長、データ属性
暗号処理	対象秘密情報、処理の種類(暗号化、復号、認証、署名)
アプリケーション実行	対象秘密情報、アプリケーション識別番号
アプリケーションコマンド	実行中のアプリケーションに依存

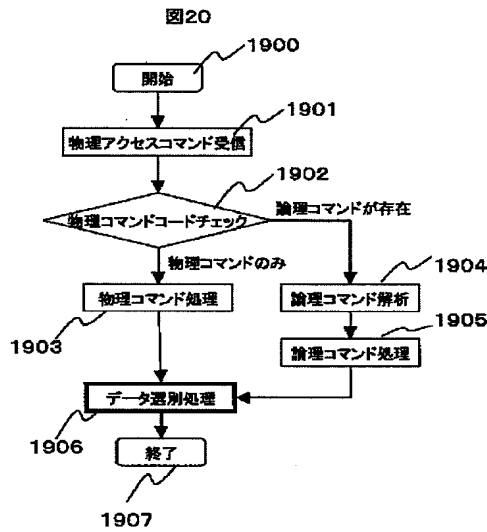
セキュリティレベル1812	説明
1	NVメモリへ格納
2	暗号化して外部メモリへ出力
3	暗号化の必要なし

【図16】

図16



【図20】



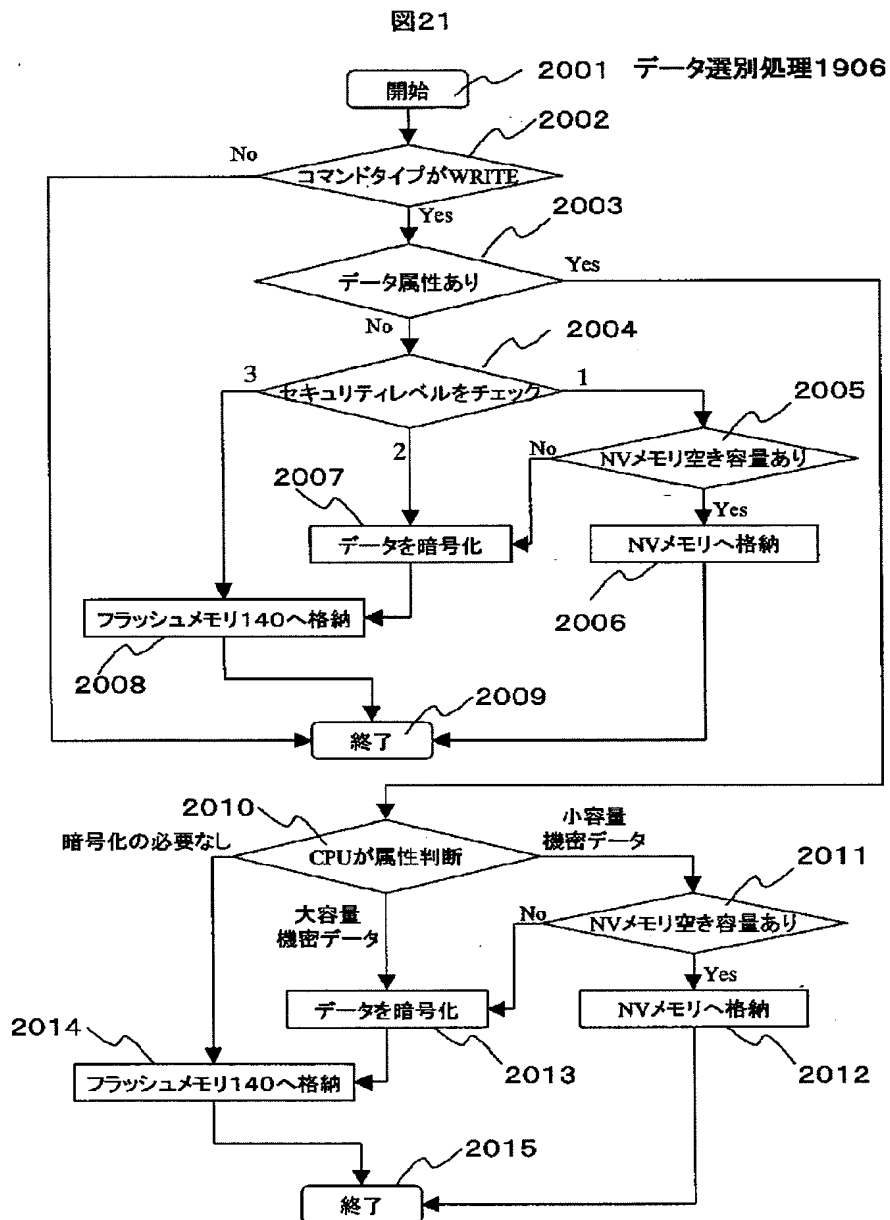
【図22】

図22

表記法規定2101

名称	表記	データの所在	意味
暗号化	$E(K, D)$	——	情報Dを鍵Kで暗号化した結果
連結	$A \parallel B$	——	情報Aと情報Bを連結した情報
コンテンツID	ContentID	——	コンテンツごとに割り当てられた番号
ルート秘密鍵	K_a	秘密情報 K_i	CAで安全に保管されている秘密鍵
メディアクラス秘密鍵	K_{mcx}	秘密情報 K_i	同一メディアクラス(ロット)のチップがその内部に秘密裏に維持する鍵
メディアクラス公開鍵	KP_{mcx}	秘密情報 K_i	K_{mcx} に対応する公開鍵
関連情報	I_{xx}	秘密情報 K_i	xx などに関連する各種情報
証明書(Certificate)	$C(K_a, KP_{xx} \parallel I_{xx})$	秘密情報 K_i	公開鍵 KP_{xx} の証明書 $KP_{xx} \parallel I_{xx} \parallel E(K_a, H(KP_{xx} \parallel I_{xx}))$
トランザクションID	TransactionID	サーバ	トランザクションごとにユニークな識別子値
セッション鍵	K_{sx}	サーバと秘密情報 K_i	通信のセッション毎に、通信エンティティ間で共有する一時的な共通鍵暗号法の鍵
メディア個別秘密鍵	K_{mx}	秘密情報 K_i	各メディアが個別に秘密裏に維持する鍵
メディア個別公開鍵	KP_{mx}	秘密情報 K_m	K_{mx} に対応する公開鍵
CRL更新日時	CRLUpdate	秘密情報 K_i	CRLを更新した日時
メディアアクセス条件	AC_m	ライセンス情報	メディア内部でのデータの扱いについて配信元が強制的に指定したアクセス条件
デコーダアクセス条件	AC_p	ライセンス情報	デコーダチップ内部でのデータの扱いについて配信元が強制的に指定したアクセス条件
コンテンツ鍵	K_c	ライセンス情報	コンテンツ毎に異なるコンテンツ暗号化鍵

【図21】



フロントページの続き

(51)Int. Cl.⁷
 G 0 6 K 19/073
 G 1 1 C 16/02
 H 0 4 L 9/08
 9/10

識別記号

F I
 G 0 6 F 9/06
 G 0 6 K 19/00
 G 1 1 C 17/00
 H 0 4 L 9/00

キーワード(参考)

6 6 0 L 5 J 1 0 4
 P
 6 0 1 P
 6 4 1
 6 0 1 A
 6 0 1 E

(72)発明者 角田 元泰
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
(72)発明者 石原 晴次
東京都小平町上水本町五丁目20番1号 株
式会社日立製作所半導体グループ内
(72)発明者 水島 永雅
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 戸塚 隆
東京都小平町上水本町五丁目20番1号 株
式会社日立製作所半導体グループ内
F ターム(参考) 5B017 AA07 BA07 CA15 CA16
5B025 AC00 AE10
5B035 AA01 AA07 AA13 BB09 BB11
BB12 CA02 CA11 CA39
5B065 BA09 PA04 PA14
5B076 BB06 FA20 FB01
5J104 AA01 AA16 EA04 EA18 JA03
NA02 NA35 NA42 PA14